UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A cellular telephone described as: Apple iPhone in a clear case, currently located in the custody of the DEA Dayton Resident Office

Case No. 3:23-mj-503

APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1) and 846	Possession with Intent to Distribute Narcotics and Conspiracy to Commit the Same

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

CALVIN BURCH (Affiliate) Digitally signed by CALVIN BURCH (Affiliate) Date: 2023.11.20 19:29:49 -05'00'

Applicant's signature

TFO Calvin Burch, DEA

Printed name and title

Sworn to before me and signed in my presence via telephone.

Date: November 21, 2023

Caroline H. Gentry
United States Magistrate Judge

City and state: Dayton, Ohio

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Calvin Burch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—specifically one (1) electronic device listed below (hereinafter – **Target Telephone)** —which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

1. An APPLE IPHONE WITH A CLEAR CASE

The **Target Telephone** is described more fully in Attachments A

2. I am a Task Force Officer (TFO) with the United States Drug Enforcement Administration (DEA), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 21, United States Code, Section 878. I have been employed as a Task Force Officer with the DEA since March 2022 and a Police Officer with the Springfield Police Division since February 2015. In 2014, I attended the Clark State Community College which consisted of training in conducting basic police operations. Since then, I have attended many hours of training including, but not limited to, drug trafficking investigations, tactical entry and vehicle arrest operations, criminal interdiction, interview/interrogation, cell phone narcotic investigations, and additional aspects of conducting investigations. Prior to beginning my assignment as a DEA TFO, I was a sworn Law

Enforcement Officer of the State of Ohio who was charged with the duty to investigate criminal activity and enforce the criminal laws of the State of Ohio. I have investigated numerous drug trafficking investigations since 2019, when I began the assignment as a narcotics investigator for the Springfield Police Division. I continue to be employed as a Springfield Police Officer.

3. I also have been involved in narcotic related arrests and executed search warrants that resulted in the seizure of narcotics. During my training, I have learned methods by which drug traffickers possess and distribute controlled substances; the manner and means in which they conceal and launder the proceeds from the distribution of controlled substances; the manner and means in which they protect their proceeds and controlled substances; and the manner in which they attempt to avoid law enforcement detection of their activities.

4. My experience as a Law Enforcement Officer/Detective with the City of Springfield Police Division in Springfield, Ohio, includes but is not limited to: physical surveillance; supervising informants during the purchases of controlled substances; debriefing persons arrested and convicted of drug trafficking offenses about their illegal activity; compiling, organizing, and analyzing precise location information (GPS data) and telephone toll data; interviewing witnesses; drafting search warrants; seeking seizure of illegal drugs and other evidence of drug violations; searching locations and seizing narcotics, "tools of trade," documents, and the monetary gains of narcotics trafficking; assisting Prosecutors in the prosecution of defendants on trial for state drug violations; and, testifying as a witness concerning the violations of State of Ohio drug laws.

5. I have participated in the preparation of affidavits in support of numerous search and arrest warrants for violations of State of Ohio criminal laws, as well as in the execution of the same. In addition, I have on numerous occasions seized contraband, conveyances, currency, drug paraphernalia, and firearms possessed or used in relation to violations of State of Ohio criminal

laws.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841 and 846 have been committed, are being committed, and will be committed by Adrian WHITE and others. There is also probable cause to believe that the information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of a crime, as well as fruits of a crime, or other items illegally possessed in relation to the following offenses exist and can be found inside the **Target Telephone** – namely: violations of 21 U.S.C. §§ 841(a)(1) and 846 (possession with intent to distribute narcotics and conspiracy to commit the same).

9. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

10. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

11. The United States, including the Drug Enforcement Administration, is conducting a criminal investigation into Adrian WHITE, William BATES, and others regarding possible violations of 21 U.S.C. §§ 841(a)(1) (possession with the intent to distribute controlled substances), 843(b) (use of a communication facility to commit a felony), and 846 (conspiracy to possess with the intent to distribute controlled substances).

12. On Thursday, November 16, 2023, at approximately 9:00 am, DEA Dayton Resident Office Task Force Officers Justin Allender, William Sanders, and I conducted surveillance on Adrian WHITE at 3179 Valerie Arms Drive, Dayton, Ohio.

13. Based on the ongoing investigation, I have learned that 3179 Valerie Arms Drive, Dayton, Ohio Unit 14 is owned by Aye White Investments LLC since December 19, 2022. Through an open source search of Aye White Investments LLC, Adrian WHITE is the owner agent of this business. Therefore I believe that when WHITE and associates are at 3179 Valerie Arms Drive, they are specifically entering Unit 14.

14. At approximately 9:58 am, I observed a Chevrolet Impala bearing the Ohio temporary license plate: R267773 arrive to 3179 Valerie Arms Drive and park in the front. After parking, TFO Burch observed William BATES exit the Impala and proceed to enter the front door of 3179 Valerie Arms Drive. I am able to identify BATES from a distance due to many hours watching BATES and looking at photos of him.

15. About ten (10) minutes later, BATES exited the front door of the apartment complex and departed in the Impala. While on surveillance, I learned that the Ohio temporary license plate R267773 is registered to William BATES.

16. At approximately 10:15 am, I observed a Kia Forte bearing the Ohio license plate JSS2994 park in front of the apartment complex. Moments later, Sonqua MCGRAW exited the vehicle; at the same time a blue Dodge Caravan bearing the Ohio temporary license plate R480257 appeared from the rear of the 3179 Valerie Arms Drive and stopped to talk to MCGRAW. While MCGRAW was talking to the driver of the Dodge Caravan, TFO Allender drove by the two and identified WHITE to be the driver and sole occupant within the Dodge Caravan.

17. Since investigating this Drug Trafficking Organization (DTO), I am already aware that Sonqua MCGRAW is the registered owner of the Kia Forte, JSS2994 and am also able to identify her from a distance from the hours of surveillance. While on surveillance, I learned that the blue Dodge Caravan being the Ohio temporary license plate R480257 is registered to Adrian WHITE.

18. At approximately 10:22 am, I observed MCGRAW getting into her Kia Forte and depart westbound on Valerie Arms Drive; at the same time, WHITE departed eastbound and ultimately traveled to the Northwest Plaza at 2901 Philadelphia Drive, Dayton. WHITE stopped at a health store and then shortly later returned 3179 Valerie Arms and parked behind the apartment complex.

19. At approximately 10:43 am, TFO Sanders observed BATES park in front of 3179 Valerie Arms Drive in the Chevrolet Impala that was previously mentioned and walk into the front door of the apartment complex, empty handed.

20. At approximately 10:51 am, TFO Sanders observed MCGRAW arrive in the previously mentioned Kia Forte, park in the front and then walk into the apartment complex with a clear tote.

21. At approximately 10:58 am, TFO Sanders observed a black Maserati, bearing the Ohio license plate KAP4968 park in front of the apartment complex. Shortly after, a heavier set, black female with long dreads exited the driver's seat and moments later got back inside the vehicle. While the female got back into the driver' seat, WHITE exited the front doors of the 3179 Valerie Arms Drive and got into the passenger's seat of the Maserati. About one (1) minute later, WHITE exited the vehicle and went back into the apartment complex.

22. At approximately 11:05 am, TFO Sanders observed BATES exit the 3179 Valerie Arms Drive with a black shoebox and placed it within his Chevrolet Impala on the passenger's side. TFO Sanders then observed BATES get into the driver's seat of the Chevrolet Impala and depart westbound. TFOs Allender, Sanders, and I then followed BATES. BATES ultimately made his way to I-70 west towards Indiana.

23. Based on the investigation into this DTO, they have connections to Indiana and supplying individuals from Indiana with multiple pounds of methamphetamine; often times utilizing shoeboxes in order to transport these narcotics. Based on the actions observed at 3179 Valerie Arms Drive and the fact that BATES was now traveling in the direction of Indiana, investigators believed BATES was transporting narcotics.

24. At approximately 11:53 am, TFO Burch was able to contact Ohio State Highway Patrol Trooper Pohlabel in reference to the ongoing investigation. At approximately 11:59 am, Trooper Pohlabel was able to conduct a traffic on the 2014 Chevrolet Impala for following too

closely on a commercial tractor trailer combination. The suspect vehicle was approximately 2- 2 ½ vehicle lengths behind the commercial unit at a speed of 70 mph.

25. During the course of this traffic stop, Trooper Pohlabel made contact with the driver who was identified as William BATES. Trooper Pohlabel ultimately utilized his canine, K9 Sahra, in order to conduct a free air sniff around the exterior of the vehicle. K9 Sahra is a certified narcotics detection canine. The canine indicated to the presence of narcotics, which then led to a search of BATES' vehicle.

26. While searching the vehicle, Trooper Pohlabel located a black shoebox on the rear passenger side floorboard of the vehicle. Within this shoebox, Trooper Pohlabel observed seven (7) ziplock baggies of containing a crystal rocklike substance, suspected of being methamphetamine. Trooper Pohlabel also observed and seized an Apple Iphone (**Target Telephone**), which was located on the center console.

27. Throughout the course of this investigation, I have administratively subpoenaed AT&T for call detail records. Each time that AT&T has responded, I reviewed the information personally and with the assistance of an analyst and together we have determined that WHITE is in frequent contact with 937-998-9056. Per law enforcement records, this number comes back to William BATES. I believe that searching the **Target Telephone** will also provide additional evidence of WHITE's involvement in his DTO.

28. Based on my training and experience, I believe that BATES was traveling to an unknown location in order to provide or sell the seven (7) ziplock baggies of containing a crystal rocklike substance, suspected of being methamphetamine. Additionally, I know that drug traffickers typically utilize cell phones in order to conduct their drug trafficking activities and keep in contact with customer and supplier of narcotics. I believe evidence of BATES drug

trafficking activities, as well as the identity of possible co-conspirators, may be stored on the **Target Telephone.**

29. The **Target Telephone** is currently in the possession of the DEA Dayton Resident Office. In my training and experience, I know that the **Target Telephone** has been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state, as they were when the **Target Telephone** first came into the possession of the DEA Dayton Resident.

30. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence of a crime - namely, Title 21 U.S.C. §§ 841(a)(1) and 846, Possession with the Intent to Distribute Controlled Substances and Conspiracy to Commit the Same - can be found within the **Target Telephone**.

TECHNICAL TERMS

1. Based on my training and experience, I use the following technical terms to convey the following meanings:

    1. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone

numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

2. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

3. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence

of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

4. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

5. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform

different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

6. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

7. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

2. Based on my training, experience, and research, I know that the **Target Telephone** has the capabilities that allow them to serve as "a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and Tablet." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

3. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

4. There is probable cause to believe that things that were once stored on the **Target Telephone** may still be stored there, for at least the following reasons:

1. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

2. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

3. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

4. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

5. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Target Telephone** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Target Telephone** because:

1. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

2. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

3. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

4. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

5. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

6. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Target Telephone** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

7. *Manner of execution.* Because this warrant seeks only permission to examine **Target Telephone** already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

8. Based on the above facts and circumstances, I submit that this affidavit supports probable cause for a search warrant authorization the examination of the **Target Telephone** described in attachments A, to seek the items described in Attachment B.

Respectfully submitted,

CALVIN BURCH (Affiliate)

Digitally signed by CALVIN BURCH (Affiliate)
Date: 2023.11.20 19:33:33 -05'00'

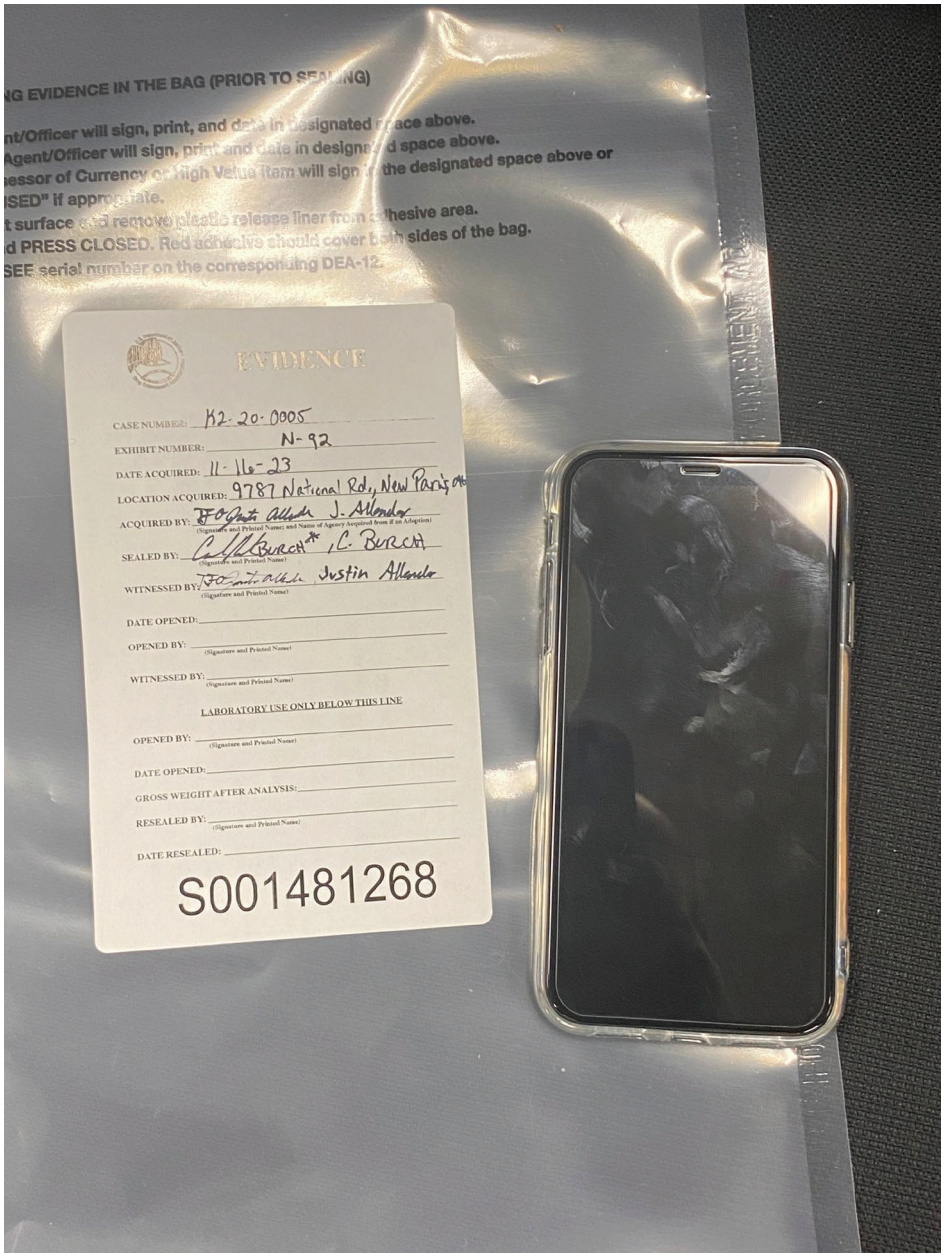
Calvin Burch
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me By telephone
on 21st day of November, 2023.

Caroline H. Gentry
United States Magistrate Judge

ATTACHMENT A

The property to be searched is an Apple iPhone with a clear case. The device is currently located in the custody of the DEA Dayton Resident Office. A picture of the seized item is listed below:



ATTACHMENT B

1. All records on the **Target Telephone** described in Attachments A, that relate to violations of 21 U.S.C. §§ 841(a)(1) and 846 (possession with intent to distribute narcotics and conspiracy to commit the same).

    a. any communications, including but not limited to: phone calls, text messages, application messages, relating to the use, possession, receipt, transportation, and/or purchase of controlled substances;

    b. any information related to sources of firearms or controlled substances (including names, addresses, phone numbers, or any other identifying information);

    c. any internet search history and browser files related to sources and possession of controlled substances;

    d. types and amounts of controlled substances possessed and/or trafficked as well as dates, places, and amounts of specific transactions;

    e. any information related to drug proceeds and the location and/or use or transfer of such proceeds:

    f. any information, including GPS location information, recording BATES' schedule or travel in connection to trafficking in controlled substances;

g. any photographs and videos, including metadata, and any other records, relating to source or possession of controlled substances; and

h. all bank records, checks, credit card bills, account information, and other financial records**.**

2. Evidence of user attribution showing who used or owned the **Target Telephone** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DEA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.